

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the
District of New Jersey

United States of America

v.

AL-FAHIM MEDINA

Case No.

21-mj-2004 (AMD)

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of 1/31/20 through on or about 2/22/20 in the county of Burlington in the
 District of New Jersey, the defendant(s) violated:

Code Section

Description of Offenses

18 U.S.C. Sections 2252A(a)(2)(A) See Attachment A
and 2252A(b)(1) and Title 18
U.S.C. Section 2

This criminal complaint is based on these facts:

See Attachment B

☒ Continued on the attached sheet.

Complainant's signature

S/A Nicholas Tranchitella, HSI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

 telephone (specify reliable electronic means).Date: 01/08/2021

Judge's signature

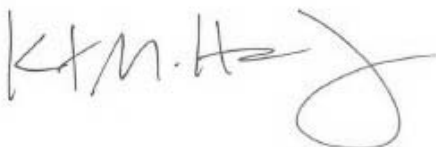
City and state: District of New Jersey

Hon. Ann Marie Donio, U.S. Magistrate Judge

Printed name and title

CONTENTS APPROVED

UNITED STATES ATTORNEY

A handwritten signature in black ink, appearing to read 'K.M. Harberg', with a large, stylized flourish at the end.

By:

KRISTEN M. HARBERG, AUSA

Date: January 7, 2021

ATTACHMENT A

From on or about January 31, 2020 through on or about February 22, 2020, in Burlington County, in the District of New Jersey and elsewhere, the defendant,

AL-FAHIM MEDINA,

did knowingly distribute child pornography, as defined in Title 18, United States Code, Section 2256(8)(A), that had been mailed, or using any means and facility of interstate and foreign commerce, shipped and transported in and affecting interstate and foreign commerce by any means, including by computer.

In violation of Title 18, United States Code, Sections 2252A(a)(2)(A) and 2252A(b)(1) and Title 18, United States Code, Section 2.

ATTACHMENT B

I, Nicholas Tranchitella, am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations. I have knowledge of the following facts based upon my own investigation, my discussions with other law enforcement personnel, and my review of evidence and documents. Because this affidavit is being submitted for the sole purpose of establishing probable cause to support the issuance of a complaint, I have not included each and every fact known to the government concerning this matter. Where statements of others are set forth herein, these statements are related in substance and in part. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged.

1. On or about January 31, 2020, a Homeland Security Investigations undercover agent (hereafter, “the UC”) identified a Twitter social media profile page bearing the title “Blackfirepv” and username “@blackfirepv” which advertised pornography for sale. Specifically, the advertisement stated, “...raunch no limits Perv. \$5 links for sale...” On the same page, the Twitter profile provided the usernames “blackfirepv” and “Blackstarpv” in connection with two internet-based chat applications.

2. On or about January 31, 2020, the UC communicated with “Blackstarpv” on one of the secure, encrypted, social media messaging and chat applications referenced above in Paragraph 1 (hereafter, “the Chat Application”). In the ensuing exchange, “Blackstarpv” confirmed that he/she was selling internet links for \$5.00 each. “Blackstarpv” provided the UC with screenshots of video file thumbnails connected to his/her advertised links. The UC reviewed those thumbnails and discovered several depictions of content constituting child pornography.

3. On February 20, 21, and 22, 2020, “Blackstarpv” and the UC communicated on the Chat Application, and “Blackstarpv” agreed to sell four links to the UC for a total of \$20.00. “Blackstarpv” told the UC that the UC could pay him/her via Venmo under account name “@black-stars.”

4. On February 22, 2020, the UC attempted to send \$20.00 to “Blackstarpv” via Venmo, but the UC had technical difficulties with Venmo, and the payment did not go through. The UC accordingly asked “Blackstarpv,” via the Chat Application, if he/she could send payment via PayPal instead. “Blackstarpv” agreed, and stated that his/her PayPal account was harleybarb1998@gmail.com. “Blackstarpv” provided the UC with some more screenshots of video file thumbnails connected to the advertised links. The UC reviewed those screenshots and determined that they contained approximately 70 videos constituting child pornography. The UC sent \$20.00 to “Blackstarpv’s” PayPal account, and after verifying that the funds had been deposited into the PayPal account, “Blackstarpv” sent the UC, via the Chat Application, four links to cloud storage website addresses. The UC accessed all four website addresses and determined that three of them contained video files constituting child pornography.

5. In the meantime, summonses were served on Twitter, Inc., PayPal, Inc., and Venmo, requesting subscriber information, IP address records, and transaction histories. PayPal, Inc., responded that the account holder of the harleybarb1998@gmail.com PayPal account was Al-Fahim Medina (hereafter “DEFENDANT MEDINA”), of 77 Tidewater Lane, Willingboro, New Jersey (hereafter “THE WILLINGBORO RESIDENCE”), phone number 609-515-7379. Venmo responded that the account holder of the @black-Stars Venmo account listed his/her phone number as 609- 515-7379, and e-mail address as daichi7606@gmail.com. Additionally, Venmo identified four electronic devices connected to the @black-Stars account through Internet

Protocol (IP) address 76.116.94.207. A subsequent query of phone number 609-515-7379 confirmed it to be a registered Metro, PCS exchange subscribed to by DEFENDANT MEDINA at THE WILLINGBORO RESIDENCE. Twitter responded that the account holder of the blackfirepv Twitter account listed daichi7606@gmail.com as his/her email account. Additionally, Twitter login data confirmed the user account was most recently accessed from the IP address 76.116.94.207. Comcast Cable Communications identified DEFENDANT MEDINA'S mother, Millie Medina, of THE WILLINGBORO RESIDENCE, as the account holder and associated with IP address 76.116.94.207. The New Jersey State Division of Motor Vehicles database confirmed that DEFENDANT MEDINA resided at THE WILLINGBORO RESIDENCE.

6. On or about June 12, 2020, a federal search warrant was executed at THE WILLINGBORO RESIDENCE. During that warrant execution, I encountered and identified DEFENDANT MEDINA. In a consensually recorded, non-custodial interview, DEFENDANT MEDINA affirmed his full-time residency within THE WILLINGBORO RESIDENCE. Additionally, DEFENDANT MEDINA acknowledged owning an iPhone XR, iPhone 6S, iPad, and ZTE Cellular Phone located within THE WILLINGBORO RESIDENCE. When informed as to the nature of law enforcement's investigation, DEFENDANT MEDINA admitted to knowingly distributing child pornography. Further, DEFENDANT MEDINA claimed ownership of the subject Twitter profile used to advertise his content, admitted to creating PayPal and Venmo accounts to receive payment for that content, and acknowledged maintaining the Google account daichi7606@gmail.com as his primary e-mail address. Simultaneous to my interview of DEFENDANT MEDINA, law enforcement encountered and identified DEFENDANT MEDINA's mother, Milagros Medina within THE WILLINGBORO

RESIDENCE. During a conversation with Mrs. Medina, law enforcement observed a MacBook Pro laptop computer. When questioned regarding the computer, Mrs. Medina claimed ownership of the device, further stating “Al also uses it sometimes,” referring to DEFENDANT MEDINA. Upon conclusion of the warrant execution, DEFENDANT MEDINA’s electronic devices and Milagros Medina’s MacBook Pro laptop computer were seized for forensic examination.

7. Between July 2020 and October 2020, the items seized from THE WILLINGBORO RESIDENCE were forensically examined. Based on those examinations, over 22,900 files of content constituting child pornography were collectively identified between the MacBook Pro laptop computer, Apple iPhone 6S and Apple iPad. A cross-reference of the content contained within those devices against the videos transmitted by “Blackstarpv” to the UC yielded six positive matches across two separate devices (five on the MacBook Pro laptop and one on the iPhone 6s). Those files are identified below and are summarized as follows.

- a. 2018-11-28 12.53.36.mp4 (directly recovered from within the MacBook Pro laptop): This video, which is :10 in length, depicts an adult male’s erect penis penetrating an infant male child’s anus.
- b. 2018-11-17 20.05.58.mp4 (directly recovered from within the MacBook Pro laptop): This video, which is 1:19 in length, depicts an adult male violently sodomizing an infant child by penetrating the child’s anus with his erect penis while the infant screams in pain.
- c. “rythmofthefuck” (recovered from a hyperlink within the MacBook Pro Laptop): This video, which is :26 in length, depicts a prepubescent adolescent male being sodomized by an adult male. Specifically, it shows an adult male thrusting his erect penis into the child’s anus while the child makes faces and noises which show that he is in pain.
- d. Video0237.mp4” (recovered from a hyperlink within the MacBook Pro Laptop): This video, which is 10:48 in length, depicts a naked prepubescent adolescent male performing fellatio and masturbating an adult male’s erect penis.
- e. Video0233_Xvid.avi” (recovered from a hyperlink within the MacBook Pro Laptop): This video, which is 1:26 in length, depicts a prepubescent adolescent male performing fellatio upon an adult male’s erect penis while he is gagging and making

sounds of discomfort and distress.

- f. Video0233_Xvid.avi” (recovered from a hyperlink within the iPhone 6S): (Same as above, in Paragraph 7f).

8. In light of the information learned by me throughout this investigation, including the fact that DEFENDANT MEDINA owned a social media profile used to advertise pornographic content for sale, that DEFENDANT MEDINA electronically communicated with an undercover agent for the purpose of transmitting child pornography, that DEFENDANT MEDINA transmitted videos containing child pornography to facilitate a monetary transaction, that DEFENDANT MEDINA established at least two separate online payment systems to receive compensation in return for the distribution of child pornography, that multiple devices registered to one of those payment systems were linked to an IP address assigned to the WILLINGBORO RESIDENCE, that examinations of electronic devices lawfully seized from the WILLINGBORO RESIDENCE resulted in the discovery and forensic confirmation of the videos containing child pornography transmitted by DEFENDANT MEDINA to an undercover agent, and that DEFENDANT MEDINA confessed to conducting all of the above actions, probable cause exists to believe that the crime of distribution of child pornography has been committed, and that DEFENDANT MEDINA is the person who committed that crime.